Technical Note

Sharing is optimal

Agostino Cortesi *, Gilberto Filé

*Corresponding author. Tel.: +39 41 290 8428; fax: +39 41 290 8419; e-mail: cortesi@dsci.unive.it.

Universita Ca Foscari, Computer Science Department, Via Torino 155, 30170 Mestre-Venezia, Italy

Received 13 January 1998; received in revised form 4 May 1998; accepted 17 August 1998

Abstract

One of the most popular abstract domains used for the analysis of logic programs is the domain Sharing which expresses the fact that computed substitutions bind variables to terms containing common variables. Despite the fact that this domain is widely used and studied, it is not yet known whether its abstract operations are complete or at least optimal. We solve this open question showing that the operations of lub and projection of Sharing are complete (and thus optimal), whereas that of unification is optimal, but not complete.

(C) 1999 Elsevier Science Inc. All rights reserved.

Keywords: Static analysis; Abstract interpretation

1. Introduction

Abstract interpretation [1] is a general framework for defining and relating different semantics of transition systems. The most popular application of abstract interpretation is the design of data flow analysis for programming languages. Many data flow analyses have been designed for logic programs and often these analyses have the goal of inferring variable sharing information. This information is useful for many purposes: AND-parallelism [2], freeness [3], program transformation [4,5]. Probably the most popular domain for inferring sharing information is Sharing [6]. Despite the number of applications of Sharing and of studies of its properties [7–10], a fundamental property of Sharing is not yet known: whether its operations are complete [1,11] or at least optimal [1].

We answer this question here showing that the operations lub and projection of Sharing are complete (and thus optimal), whereas the unification operation is only optimal and not complete. To this end we also show the correctness of all three operations of Sharing. As a matter of fact, the correctness of the unification of Sharing has been already shown in Refs. [6,10], but in these works the domain is different from that considered here and thus we give the full proof of this result.
too. It is worth mentioning that, in order to give a precise foundation to our results, we consider here an important point that arises when dealing with the concrete unification and that is often neglected: do our results depend on a particular concrete unification algorithm? We show, exploiting a result of [12], that as long as idempotent most general unifiers (mgus) are considered, the sharing does not depend on which mgu is considered.

The paper is organized as follows. Section 2 recalls some preliminary definitions. In Sections 3 and 4 the concrete interpretation Resub and the abstract interpretation Sharing are introduced, each with its three operations: lub, projection and unification. In Section 5 we show that lub and projection of Sharing are complete and in Section 6 we show that abstract unification is optimal (but not complete). Finally, Section 7 discusses recent related works, in particular [9,10], and concludes.

2. Preliminaries

2.1. Substitutions

Let V be a countable set of variables, FP(V) be the set of finite subsets of variables of V, and TV,G be the set of finite terms over V and an alphabet of function symbols G. A substitution σ is a function in V → TV,G such that σ(x) ≠ x only for a finite number of variables x. The set of support and the variable range of σ are given by supp(σ) = {x | σ(x) ≠ x} and var-range(σ) = \{Var(σx) | x ∈ supp(σ)\}, where Var(t) denotes the set of variables occurring in t. The set of variables occurring in σ is Var(σ) = supp(σ) \cup var-range(σ). A substitution may be specified by listing its nontrivial bindings, viz., σ = {x/σ(x) | x ∈ supp(σ)}. Given two substitutions σ1 and σ2, their composition, denoted σ2 \circ σ1, is {x/σ2(σ1(x)) | x ∈ supp(σ1) and σ2(σ1(x)) ≠ x} \cup {y/σ2(y) | y ∈ supp(σ2) \setminus supp(σ1)}. A substitution σ is idempotent when σ \circ σ = σ. It is well-known that σ is idempotent iff supp(σ) \cap var-range(σ) = ∅.

If there exists θ such that σ2 = θ \circ σ1, then σ1 is more general than σ2. Let E = {t1 = s1, ..., tk = sk} be a set of term equations. If σ makes σ(t1) syntactically identical to σ(s1) for each (tk = sk) ∈ E, σ is called a unifier of E.

A most general unifier of E, mgu(E), is an idempotent unifier of E that is more general than all other unifiers of E. The set E is in solved form if it has the form {x1 = t1, ..., xn = tn} where each xi is a distinct variable occurring in none of the terms ti. In this case, the substitution σ = {x1/t1, ..., xn/tn} is an idempotent mgu of E. Any idempotent substitution σ is an mgu of the corresponding set of equations in solved form, denote by Eq(σ).

We write Subst for the set of idempotent substitutions. Although Subst is not closed under composition, in a step of the execution of a logic program in which θ \circ σ is constructed, it is always the case that, var-range(θ) \cap supp(σ) = ∅, which, provided that θ and σ are idempotent, ensures that θ \circ σ is also idempotent.

2.2. Abstract interpretations

According to [1], a data-flow analysis for a programming language L is a nonstandard (abstract) semantics of L. Both the standard and an abstract semantics of L are obtained interpreting a generic semantics, where such an interpretation con-
sists of a domain of data-descriptions and of some operations on these data-descriptions.

Let us recall some basic definitions [1,13]. Let \( C \) and \( D \) be complete lattices. Two functions \( \gamma_{DC} : D \rightarrow C \) and \( \alpha_{DC} : C \rightarrow D \) form a Galois connection between \( D \) and \( C \) if

\[
\forall c \in C \text{ and } \forall d \in D : \quad \alpha_{DC}(c) \sqsubseteq_D d \iff c \sqsubseteq_C \gamma_{DC}(d).
\]

The function \( \gamma_{DC} \) is called concretization and \( \alpha_{DC} \) is called abstraction. They are said to be adjoint because one is determined by the other [13]. For instance, \( \forall d \in D, \gamma_{DC}(d) = \bigcup_c \{ c \mid c \in C, \alpha_D(c) \sqsubseteq_D d \} \). The dual relation holds for \( \alpha_{DC} \). This definition is equivalent to requiring that concretization and abstraction are monotonic and that the following two conditions hold: \( \forall c \in C, \gamma_{DC}(\alpha_{CD}(c)) \sqsupseteq_C c \) and \( \forall d \in D, \alpha_{CD}(\gamma_{DC}(d)) \sqsubseteq_D d \).

A Galois connection is said to be a Galois insertion when \( \gamma_{DC} \) is injective or, equivalently, when \( \alpha_{CD} \) is onto. In this case, \( \forall d \in D, \alpha_{CD}(\gamma_{DC}(d)) = d \).

Assume that an abstract operation \( \mu \) corresponds to a concrete one \( op \). We say that \( \mu \) is correct with respect to \( op \) when

\[
\forall d \in D, \mu(d) \sqsupseteq_D \alpha_{CD}(op(\gamma_{DC}(d)))).
\]

The operation \( \mu \) is optimal when the above disequation becomes an equality. In [1,11], the stronger notion of completeness of an abstract operation is introduced and discussed. The abstract operation \( \mu \) is complete when

\[
\forall c \in C, \alpha_{CD}(op(c)) = \mu(\alpha_{CD}(c)).
\]

Obviously, an optimal abstract operation is also correct. When there is a Galois insertion, it is also easy to see that a complete operation is also optimal, but the converse is not true.

3. The concrete interpretation \( \langle \mathbb{R}_{\text{sub}}, \sqcup_{\mathbb{R}}, \pi_{\mathbb{R}}, U_{\mathbb{R}} \rangle \)

Before introducing the concrete interpretation, some explanations are due. In this paper we adopt the classical abstract interpretation approach of [1,13]. In this approach, both the concrete and the abstract semantics are obtained by instantiating a common generic semantics. This approach has the advantage of allowing modular correctness proofs: instead of proving the correctness (optimality, completeness) of the whole abstract semantics w.r.t. the concrete one (for instance the SLD semantics), one can show the correctness (optimality, completeness) of each basic operation.

This approach has two important consequences on the concrete interpretation [14] adopted here. The elements of this domain consist of pairs where the first component is a set of substitutions (as usual) and the second component is a finite set of variables that specifies the variables of interest, i.e., the variables the analysis wants to deals with. This second component is needed in order to account, in the concrete domain, for the fact that the abstract semantics computes values concerning only finite sets of variables (in general, the variables of the clauses of the analyzed program).

The second consequence is that the concrete interpretation includes also a projection operation. This operation is the concrete counterpart of the abstract projection which, on the contrary, has a very important role in making the abstract semantics finitely computable.
Although non-standard, this choice of concrete domain allows to use an uniform notation for concrete/abstract values and operations, and this is the reason we adopt it [14,7,8]. Moreover, it enjoys two positive features: its values are almost identical to the sets of substitutions computed by Prolog programs, and the projection operation is very simple, matching the feeling that projection does not belong to the concrete semantics, but it is "inherited" from the abstract semantics, where it is necessary for achieving finiteness, as said above.

3.1. Domain

The set $\text{Rsub} = [\varphi(\text{Subst}) \times \text{FP}(V)] \cup \{\top_{RS}, \bot_{RS}\}$. $\text{Rsub}$ stands for restricted substitutions. The partial order of $\text{Rsub}$ is defined as follows. $\top_{RS}$ is the largest element, $\bot_{RS}$ is the smallest one, whereas $[\Sigma_1, U_1] \sqsubseteq_{RS} [\Sigma_2, U_2]$ iff $U_1 = U_2$ and $\Sigma_1 \subseteq \Sigma_2$.

3.2. Least upper bound and greatest lower bound

The operation $\sqcup_{RS}$, which produces the least upper bound of two elements of $\text{Rsub}$, is as follows: for any $k \in \text{Rsub}$, $\top_{RS} \sqcup_{RS} k = \top_{RS}$, $\bot_{RS} \sqcup_{RS} k = k$, whereas

$$[\Sigma_1, U_1] \sqcup_{RS} [\Sigma_2, U_2] = \begin{cases} [\Sigma_1 \cup \Sigma_2, U_1] & \text{if } U_1 = U_2, \\ \top_{RS} & \text{otherwise}. \end{cases}$$

The greatest lower bound is defined on non-trivial elements by $[\Sigma_1, U] \sqcap_{RS} [\Sigma_2, U] = [\Sigma_1 \cap \Sigma_2, U]$. In the other cases, it is $\bot_{RS}$. $\text{Rsub}$ is a complete lattice w.r.t. $\sqsubseteq_{RS}$.

3.3. Projection

The concrete projection $\pi_{RS}$ is the identity on the first argument when this is either $\top_{RS}$ or $\bot_{RS}$, otherwise it is

$$\pi_{RS} : \text{Rsub} \times \text{FP}(V) \to \text{Rsub}$$

$$([\Sigma, U_1], U_2) \mapsto [\Sigma, U_1 \cap U_2].$$

3.4. Unification

A unique operation [14] is considered that accounts for both forward and backward unifications. Its first argument is the set of substitutions computed at calling time, the second one is the set of substitution computed when returning from the call, and the third one is a (idempotent) $\text{mgf}$ of the two atoms that are unified through the call. For using this operation as forward unification it suffices to set the second argument to the identity substitution. In order to define the concrete unification $U_{RS}$, it is convenient to introduce first the following function $u_{RS}$:

$$u_{RS} : \text{Subst} \times \text{Subst} \times \text{Subst} \to \text{Subst},$$

$$(\sigma_1, \sigma_2, \delta) \mapsto \text{mgf}(\text{Eq}(\sigma_1) \cup \text{Eq}(\sigma_2) \cup \text{Eq}(\delta)).$$

$U_{RS}$ is strict: if either of the first two arguments is $\bot_{RS}$, the result is $\bot_{RS}$. Otherwise, if one of these is $\top_{RS}$, the result is $\top_{RS}$. The other cases are as follows: assume that
\( \text{Var}(\delta) \subseteq U_1 \cup U_2; \) then

\[
U_{\text{Rsub}}: \text{Rsub} \times \text{Rsub} \times \text{Subst} \rightarrow \text{Rsub},
\]

\[
([\Sigma_1, U_1], [\Sigma_2, U_2], \delta) \mapsto \{ u_{\text{Rsub}}(\sigma_1, \sigma_2, \delta) \mid \text{where } \sigma_1 \in \Sigma_1, \sigma_2 \in \Sigma_2,
\]

\[
\text{and } \text{Var}(\sigma_1) \cap \text{Var}(\sigma_2) = \emptyset, \ U_1 \cup U_2).
\]

Notice that \( \sigma_1 \) and \( \sigma_2 \) are required to be renamed apart. Intuitively, this works because \( \sigma_1 \) deals with the variables of the calling clause whereas \( \sigma_2 \) with those of the called clause only.

4. The abstract interpretation \( \langle \text{Sharing}, \sqcup_{\text{Sh}}, \pi_{\text{Sh}}, U_{\text{Sh}} \rangle \)

4.1. Domain

The abstract domain \( \text{Sharing} \) has been proposed by Jacobs and Langen in Ref. [6] in order to represent variable aliasing, covering, and groundness. Here we present a slightly different domain wrt the original proposal in that our domain shows explicitly the variables of interest [7,8]. This is necessary in order to use this domain in a real static analysis in which values on different sets of variables (for instance, the variables of the clauses of the analyzed program) are generally computed.

\[
\text{Sharing} = \{ [A, U] \mid A \subseteq \wp(U), (A \neq \emptyset \Rightarrow \emptyset \in A), U \in \text{FP}(V) \} \cup \{ T_{\text{Sh}}, \bot_{\text{Sh}} \}.
\]

\( \text{Sharing} \) is partially ordered: \( T_{\text{Sh}} \) is the largest element and \( \bot \) is the smallest one; for the other elements, \( [A_1, U_1], \sqsubseteq_{\text{Sh}} [A_2, U_2] \) iff \( U_1 = U_2 \) and \( A_1 \subseteq A_2 \).

4.2. Least upper bound and greatest lower bound

The least upper bound of any two elements \( [A_1, U_1] \) and \( [A_2, U_2] \) is defined by

\[
[A_1, U_1] \sqcup_{\text{Sh}} [A_2, U_2] = \begin{cases} [A_1 \cup A_2, U_1] & \text{if } U_1 = U_2, \\ T_{\text{Sh}} & \text{otherwise.} \end{cases}
\]

The greatest lower bound, if \( U_1 = U_2 = U \) is \( [A_1 \cap A_2, U] \). Otherwise, it is \( \bot_{\text{Sh}} \). The domain \( \text{Sharing} \) is a complete lattice w.r.t. \( \sqsubseteq_{\text{Sh}} \).

4.3. Abstraction

Let for any \( y \in V, \text{occ}(\sigma, y) = \{ z \in V \mid y \in \text{Var}(\sigma(z)) \} \). The abstraction function between \( \text{Sharing} \) and \( \text{Rsub} \) maps \( \bot_{\text{Rsub}} \) to \( \bot_{\text{Sh}} \) and \( T_{\text{Rsub}} \) to \( T_{\text{Sh}} \), whereas it is defined on non-trivial elements by

\[
\alpha_{R_{\text{Sh}}}(c) = \begin{cases} \text{if } c = ([\sigma], U) & \text{then } [\text{occ}(\sigma, y) \cap U | y \in V], U], \\ \text{if } c = ([\Sigma, U) & \text{then } \sqcup_{\text{Sh}} \{ \alpha_{R_{\text{Sh}}}(\{ [\sigma], U) | \sigma \in \Sigma \} \}
\end{cases}
\]

Intuitively, an element of the first component of \( \alpha_{R_{\text{Sh}}}(\{ [\sigma], U) \) is a set of variables in \( U \) that under \( \sigma \) share the same variable. Observe that a variable of \( U \) is ground in \( [A, U] \) iff it does not appear in any set of the abstract state. Clearly, \( \alpha_{R_{\text{Sh}}} \) is monotonic. In order to show that it admits an adjoint function and that the two functions form a Galois connection, it suffices by Ref. [13] to show the following result.
Proposition 4.1. The function $\alpha_{R, Sh}$ is join-complete, i.e.,

$$\forall X \subseteq \text{Rsub}, \quad \alpha_{R, Sh}(\bigcup_{i=1}^{n} X) = \bigcup_{i=1}^{n} \alpha_{R, Sh}(x) \mid x \in X.$$ 

Proof. The limit cases in which $X$ is empty or it contains $\tau_{R, s}$, or it consists of $\perp_{R, s}$ only, are immediate. Then, assume that $X$ contains some pairs $[\Sigma, U]$. All these pairs must have equal second component, otherwise both sides of the equation are trivially $\tau_{R, s}$. Then, it is sufficient to remind the definition of $\alpha_{R, Sh}$ to conclude. $\square$

The adjoint function of $\alpha_{R, Sh}$ is:

$$\gamma_{Sh, R}([A, U]) = \bigcup_{[\Sigma, U] \in \text{Rsub}} \{ [\Sigma, U] \subseteq \alpha_{R, Sh}([\Sigma, U]) \}.$$ 

Actually, $\alpha_{R, Sh}$ and $\gamma_{Sh, R}$ define a Galois insertion between $\text{Rsub}$ and Sharing. In fact the following Proposition shows that $\alpha_{R, Sh}$ is onto.

Proposition 4.2. For any $[A, U] \in \text{Sharing}$, there exists $\sigma \in \text{Subst}$ such that $\alpha_{R, Sh}([\{\sigma\}, U]) = [A, U]$.

Proof. Let $A = \{B_1, \ldots, B_m\}$. Consider $y_1, \ldots, y_m \in V \setminus U$. For each $x \in U$, let $I_x = \{i \mid 1 \leq i \leq m, x \in B_i\}$. The substitution $\sigma$ is defined by:

$$\sigma(x) = \begin{cases} 
  f(y_1, \ldots, y_k) & \text{if } I_x = \{j_1, \ldots, j_k\}, \\
  a & \text{if } I_x = \emptyset.
\end{cases}$$

It is easy to check that for such a $\sigma$ it holds $\alpha_{R, Sh}([\{\sigma\}, U]) = [A, U]$. $\square$

Example 4.1. Let us illustrate the proposition above by a simple example. Let $[A, U]$ be an element of Sharing with $U = \{x_1, x_2, x_3, x_4\}$, and $A = \{\emptyset, \{x_1, x_2, x_3\}, \{x_2, x_3\}, \{x_1, x_3\}, \{x_3\}\}$. The substitution $\sigma$ obtained according to Proposition 4.2 is based on the following correspondence between elements in $A$ and variables in $V \setminus U$.

$$\{x_1, x_2, x_3\}, \{x_2, x_3\}, \{x_1, x_3\}, \{x_3\}.$$ 

The resulting substitution is

$$\sigma = \{x_1/f(y_1, y_3), x_2/f(y_1, y_2), x_3/f(y_1, y_2, y_3, y_4), x_4/a\}.$$ 

4.4. Projection

In Sharing Projection is the identity on $\perp_{Sh}$ and $\tau_{Sh}$, whereas in the other cases it is defined through set-intersection:

$$\pi_{Sh} : \text{Sharing} \times \text{FP}(V) \rightarrow \text{Sharing} \quad \left( [A_1, U_1], [A_2, U_2] \rightarrow [\{B \cap U_2 \mid B \in A_1\}, U_1 \cap U_2] \right)$$

4.5. Unification

Some auxiliary functions are useful [6] in order to define the abstract unification function $U_{Sh}$:

- The closure under union of $A \in \varphi(\varphi(V))$, denoted $A^*$, is the smallest superset of $A$ satisfying $X \in A^* \land Y \in A^* \rightarrow (X \cup Y) \in A^*$. 

• The component of $A \in \varphi(\varphi(V))$ that is relevant to a term $t$, denoted $rel(A, t)$, is the set $\{S \in A \mid Var(t) \cap S \neq \emptyset\}$.

• If $A, A' \in \varphi(\varphi(V))$, the cross product $A \otimes A'$ is $\{(S \cup S') \mid S \in A, S' \in A'\}$.

• The basic unification step is performed by

$$u_{sh} : \varphi(\varphi(V)) \times Subst \rightarrow \varphi(\varphi(V))$$

$$\forall A_0 \in \varphi(\varphi(V)), \forall \delta \in Subst, \delta = \{x_1/t_1, \ldots, x_m/t_m\}$$

$$u_{sh}(A_0, \delta) = amgu.args([x_1, \ldots, x_m], [t_1, \ldots, t_m], A_0)$$

$$amgu.args([\_], [\_], B) = B$$

$$amgu.args([x_1 \mid x_1], [t_1 \mid t_1], B) = amgu.args(\_\_I, t_1, amgu(x_1, t_1, B))$$

$$amgu(x, t, B) = (B - (rel(x, B) \cup rel(t, B))) \cup (rel(x, B) \otimes rel(t, B))$$

• The backward/forward unification $U_{sh}$ is defined as follows. Let $[A, U], [A', U'] \in$ Sharing, with $U \cap U' = \emptyset$, and let $\delta \in Subst$ with $Var(\delta) \subseteq U \cup U'$.

$$U_{sh} : \text{Sharing} \times \text{Sharing} \times Subst \rightarrow \text{Sharing}$$

$$U_{sh}([A, U], [A', U'], \delta) = [u_{sh}(A \cup A', \delta), U \cup U'].$$

5. Lub and projection of sharing are complete

Correctness of least upper bound and projection operations have been proven, in a different setting, in Ref. [10] (see Section 7). Here, we show a stronger result: that these operations are complete too. Completeness of lub operation follows immediately from Proposition 4.1.

Theorem 5.1. The lub of Sharing is complete.

Theorem 5.2. $\pi_{sh}$ is complete with respect to $\pi_{rs}$, i.e., $\forall c \in R_{\text{sub}}$ and $U_2 \in FP(V)$,

$$\pi_{rs}(\pi_{rs}(c, U_2)) = \pi_{sh}(\pi_{rs}(c, U_2)).$$

Proof. If $c$ is either $\top_{rs}$ or $\bot_{rs}$, the result follows from the definition. Otherwise, consider $c = [\Sigma, U_1]$. We get

$$\pi_{rs}(\pi_{rs}([\Sigma, U_1], U_2)) = \pi_{rs}([\Sigma, U_1 \cap U_2])$$

by definition of $\pi_{rs}$.

$$= [\{occ(\sigma, y) \cap (U_1 \cap U_2) \mid y \in V, \sigma \in \Sigma\}, U_1 \cap U_2]$$

by definition of $\pi_{rs, sh}$.

$$= \pi_{sh}([\{occ(\sigma, y) \cap U_1 \mid y \in V, \sigma \in \Sigma\}, U_2])$$

by definition of $\pi_{sh}$.

$$= \pi_{sh}(\pi_{rs}(\Sigma, U_1), U_2)$$

by definition of $\pi_{rs, sh}$.

.
6. Unification of Sharing is optimal

This Section is organized as follows. First we show that, when computing a mgu of a set of equations $E$, all idempotent mgu's of $E$ carry the same sharing information. Thus the actual unification algorithm used has no effect on the sharing information as long as idempotent mgu's are computed. After this, we prepare the background for the optimality proof. First some notation is fixed and some technical facts are proven. Then, it is shown that $U_{ss}$ is correct and optimal w.r.t. $U_{Rs}$, but not complete.

6.1. Idempotent mgu's and sharing

In Section 3 of Ref. [12] the following result is shown:

**Theorem 6.1.** Two idempotent mgu's $\mu_1$ and $\mu_2$ of some set of equations $E$ satisfy the following two conditions:
1. $\text{Var}(\mu_1) = \text{Var}(\mu_2)$;
2. There is $\{x_1/y_1, \ldots, x_n/y_n\} \subseteq \mu_1$, with all the $y_i$ distinct, such that $\mu_2 = \{y_1/x_1, \ldots, y_n/x_n\} \circ \mu_1$.

From this result it is easy to show the following theorem.

**Theorem 6.2.** Let $\mu_1$ and $\mu_2$ be two idempotent mgu's of the same equation set. For any $U \in FP(V)$, $\alpha_{Rs \text{ sh}}([\{\mu_1\}, U]) = \alpha_{Rs \text{ sh}}([\{\mu_2\}, U])$.

**Proof.** When $U = \text{Var}(\mu_1)$ (recall that by point (1) of Theorem 6.1, $\text{Var}(\mu_1) = \text{Var}(\mu_2)$), the result follows immediately from Theorem 6.1, point (2). When $U \neq \text{Var}(\mu_1)$, just use the definition of $\alpha_{Rs \text{ sh}}$. □

6.2. Notation

In what follows, let $[A_1, U_1]$ and $[A_2, U_2] \in \text{Sharing}$ with $U_1 \cap U_2 = \emptyset$. Let also $R_0 = A_1 \cup A_2$ and $U_0 = U_1 \cup U_2$ and $\delta = \{x_1/t_1, \ldots, x_n/t_n\} \in \text{Subst}$ such that $\text{Var}(\delta) \subseteq U_0$. Recall that

$U_{ss}([A_1, U_1], [A_2, U_2], \delta) = [u_{ss}(R_0, \delta), U_0]$.

The operation $u_{ss}(R_0, \delta)$ treats the bindings of $\delta$ one at the time. We denote by $R_i$ the subset of $\varphi(U_0)$ computed after having handled the first $i$ bindings. The operation $u_{ss}$ generates sets of variables by taking the union of already present sets. Observing the computation of $u_{ss}(R_0, \delta)$ one can reconstruct which elements of $R_0$ are unioned in order to generate each element of $R_s$. 1 If an element of $R_s$ is generated in several ways, just any one of them will be considered.

In what follows we will consider $S \in R_s$ and assume that it is generated by taking the union of $K = \{B_1, \ldots, B_k\} \subseteq R_0$. Clearly, if $k$ is 1 then $S = B_1 \in R_0$.

---

1 More precisely, one could mimic the computation of $u_{ss}(R_0, \delta)$ computing $\{B_1, \ldots, B_k\}$ whenever that function computes $\cup_{i \in [1, k]} B_i$. 
6.3. Technical results

Assume the notation fixed above. $K$ satisfies the following 3 facts:

**Fact 1.** \( \forall i \in [1, n], x_i \in S \iff S \cap \text{Var}(t_i) \neq \emptyset. \)

**Fact 2.** If \( S \not\subseteq R_0 \) then \( \forall j \in [1, k], \exists i \in [1, n] \) such that \( B_j \cap \text{Var}(x_i) = t_i \neq \emptyset. \)

**Fact 3.** Let us define the following relation \( \mathcal{R} \) between elements of \( K \): \( B_i \mathcal{R} B_j \) if and only if there exists \( l \in [1, n] \), such that \( B_i \cap \text{Var}(x_l) = t_i \neq \emptyset \) and \( B_j \cap \text{Var}(x_l) = t_i \neq \emptyset. \)

Let \( \mathcal{R}^+ \) be the transitive closure of \( \mathcal{R} \); then it must be that \( \forall i, j \in [1, k], B_i \mathcal{R}^+ B_j \).

**Proof of Fact 1.** (\( \Rightarrow \)) If \( x_i \in S \) then \( x_i \) appears also in \( R_i \), and then, by definition of \( U_{\text{Sh}} \), it must be that \( \cup R_{i-1} \cap \text{Var}(t_i) \neq \emptyset. \) Moreover, each element \( B \in R_i \) that contains \( x_i \), contains also a variable in \( \text{Var}(t_i) \). Thus, this must be also true for \( S \), that contains at least one of these sets. The same reasoning proves the (\( \Leftarrow \))-direction. □

**Proof of Fact 2.** It suffices to observe that if \( \exists j \in [1, k], \) such that \( \forall i \in [1, n], B_j \cap \text{Var}(x_i) = t_i \neq \emptyset, \) then, \( U_{\text{Sh}} \) could not combine \( B_j \) with any other element of \( R_0 \), and thus \( S \) could not be produced. □

**Proof of Fact 3.** Assume that there are \( i \) and \( j \in [1, k] \) such that \( B_i \mathcal{R}^+ B_j \) is false. In this case, \( K \) can be partitioned in two parts: \( K' = \{ B \in K \mid B \mathcal{R}^+ B \} \) and \( K'' = K - K' \), such that each binding of \( \delta \) has variables in common with at most one of \( \cup K' \) and \( \cup K'' \). From this, by induction on \( n \), it follows that elements of \( K' \) and \( K'' \) are never unioned in the computation of \( U_{\text{Sh}}(R_0, \delta) \). Thus, the set \( S \) (see Section 6.2) cannot belong to \( U_{\text{Sh}}(R_0, \delta) \). Contradiction. □

6.4. Correctness

As already mentioned in the Introduction, the correctness of the abstract unification of \( \text{Sharing} \) was already shown in Ref. [6]. In a different setting, also Ref. [10] proves it. However, since the domain we consider is different and for the sake of completeness, we give the full proof of this result too.

**Theorem 6.3.** The abstract unification \( U_{\text{Sh}} \) is correct with respect to \( U_{\text{RS}} \).

**Proof.** Let \( [A_1, U_1], [A_2, U_2] \in \text{Sharing} \) with \( U_1 \cap U_2 = \emptyset. \) Let also \( R_0 = A_1 \cup A_2 \) and \( U_0 = U_1 \cup U_2 \) and \( \delta = \{ x_1/t_1, \ldots, x_n/t_n \} \in \text{Subst} \) such that \( \text{Var}(\delta) \subseteq U_0 \). The claim of the Theorem is:

\[
U_{\text{Sh}}([A_1, U_1], [A_2, U_2], \delta) \equiv_{\text{Sh}} \gamma_{\text{RS}, \text{Sh}}(U_{\text{RS}}(\gamma_{\text{Sh}, \text{RS}}([A_1, U_1]), \gamma_{\text{Sh}, R_0}([A_2, U_2]), \delta)).
\]

Let for \( i \in [1, 2], \sigma_i \in \Sigma_i, \) where \( [\Sigma_i, U_i] = \gamma_{\text{Sh}, \text{RS}}([A_i, U_i]) \) such that \( \text{Var}(\sigma_1) \cap \text{Var}(\sigma_2) = \emptyset \) as required by the concrete unification, cf. Section 3.4. Because of this assumption, an (idempotent) \( \text{mgu} \) of \( \text{Eq}(\sigma_1) \cup \text{Eq}(\sigma_2) \) is simply the union of the bindings of these
two substitutions, i.e., \( \rho_0 = \sigma_1 \cup \sigma_2 \). Therefore, it is true that
\[
\mathbf{u}_{R_i}(\sigma_1, \sigma_2, \delta) = \text{mgu}(\text{Eq}(\sigma_1) \cup \text{Eq}(\sigma_2) \cup \text{Eq}(\delta))
\]

\[
= \text{mgu}(\text{Eq}(\rho_0) \cup \text{Eq}(\delta)).
\]

It is convenient for this proof to consider the following construction of this \( \text{mgu} \): let \( \text{Eq}(\delta) = \{x_1 = t_1, \ldots, x_n = t_n\} \), first we compute \( \text{mgu}(\rho_0(x_1 = t_1)) = \mu_1 \), then if \( \rho_1 = \mu_1 \circ \rho_0 \), we compute \( \text{mgu}(\rho_1(x_2 = t_2)) = \mu_2 \), then we apply \( \rho_2 = \mu_2 \circ \rho_1 \) to \( x_3 = t_3 \) and so on. At the end of this process the obtained substitution \( \rho_n \) is an idempotent \( \text{mgu} \) of \( \delta = \text{Eq}(\rho_0) \cup \text{Eq}(\delta) \) and thus, by Lemma 6.2, whatever we can prove about its sharing, this holds for any other idempotent \( \text{mgu} \) of \( \delta \).

Below, the notation fixed in Section 6.2 will be used again. In particular, the computation of \( \mathbf{u}_{\mathbf{S}_{\mathbf{R}}}(\{R_0, U_0\}, \delta) \) is performed in a way similar to that just described for \( \rho_1, \ldots, \rho_n \); the bindings of \( \delta \) are considered one at the time and \( R_i \) is the value obtained after having considered the first \( i \) bindings of \( \delta \).

We prove by induction that
\[
\forall i \in [0, n], \gamma_{\mathbf{S}_{\mathbf{R}_i}}([R_i, U_0]) \equiv_{\mathbf{R}_i} \{(\rho_i), U_0\}.
\]

From this fact the theorem follows by observing that \( \mathbf{U}_{\mathbf{S}_{\mathbf{R}}}(\{A_1, U_1\}, \{A_2, U_2\}, \delta) = \{R_n, U_0\} \), and by using the definition of Galois connection.

**Base** \((i = 0)\). From the assumption, \( \forall i \in [1, 2], \sigma_i \in \gamma_{\mathbf{S}_{\mathbf{R}_i}}(\{A_i, U_i\}) \), and \( U_1 \cap U_2 = \emptyset \). It follows that \( \{(\rho_0), U_0\} \in \gamma_{\mathbf{S}_{\mathbf{R}_0}}(\{R_0, U_0\}) \).

**Step** \((i > 0)\). Assume now that the above statement holds for \( \{R_{i-1}, U_0\} \) and \( \rho_{i-1} \), and consider \( \mu_i = \text{mgu}(\rho_{i-1}(x_i = t_i)) \) and \( \rho_i = \mu_i \circ \rho_{i-1} \).

Observe that, by the definition of the operator \( \text{occ} \), \( \text{occ}(\rho_i, y) \cap U_0 \neq \emptyset \) only for \( y \in \text{var-range}(\rho_i) \cup (U_0 \setminus \text{supp}(\rho_i)) \). Thus, we need to show that for each \( y \) either in the \( \text{var-range} \) of \( \rho_i \) or in \( U_0 \setminus \text{supp}(\rho_i) \), it is true that \( \text{occ}(\rho_i, y) \cap U_0 \in R_i \). We distinguish two cases.

1. \( y \notin \text{Var}(\rho_{i-1}(x_i = t_i)) \). This implies that \( \text{occ}(\rho_{i-1}, y) \cap \text{Var}(x_i = t_i) = \emptyset \). \((+)\)

On the one hand, from \((+)\) it follows that all the bindings of \( \rho_{i-1} \) concerning \( y \) are unchanged in \( \rho_i \). Moreover, no new binding concerning \( y \) can be added in \( \rho_i \) because \( y \notin \text{Var}(\rho_{i-1}(x_i = t_i)) \). Thus, \( \text{occ}(\rho_i, y) = \text{occ}(\rho_{i-1}, y) \).

On the other hand, \((+)\) implies that \( \text{occ}(\rho_{i-1}, y) \cap U_0 \notin \text{rel}(x_i = t_i, R_{i-1}) \) and thus, by definition of \( \mathbf{u}_{\mathbf{S}_{\mathbf{R}}} \), \( \text{occ}(\rho_{i-1}, y) \cap U_0 \) is not modified after precessing the \( i \)th binding of \( \delta \). Hence, \( \text{occ}(\rho_i, y) \cap U_0 \in R_i \).

2. \( y \in \text{Var}(\rho_{i-1}(x_i = t_i)) \). Let \( B = \text{occ}(\mu_i, y) \). Observe that \( B \neq \emptyset \) since \( \mu_i = \text{mgu}(\rho_{i-1}(x_i = t_i)) \). In \( \rho_i \), \( y \) will be shared by all the variables that in \( \rho_{i-1} \) share some variable in \( B \). More precisely,

\[
\text{occ}(\rho_i, y) \cap U_0 = \bigcup \{\text{occ}(\rho_{i-1}, w) \cap U_0 \mid w \in B\}.
\]

By induction hypothesis, all the sets \( \text{occ}(\rho_{i-1}, w), w \in B \), are in \( R_{i-1} \). In order to conclude the proof we show that \( \mathbf{u}_{\mathbf{S}_{\mathbf{R}}} \) computes their union.

Since each \( w \in B \) is in \( \text{Var}(\rho_{i-1}(x_i = t_i)) \), it must be that \( \text{occ}(\rho_{i-1}, w) \cap \text{Var}(x_i = t_i) \neq \emptyset \). Thus, since \( U_0 \supseteq \text{Var}(x_i = t_i) \), it follows that \( \text{occ}(\rho_{i-1}, w) \cap U_0 \in \text{rel}(x_i = t_i, R_{i-1}) \). This shows that all the sets \( \text{occ}(\rho_{i-1}, w) \cap U_0 \) that must be unioned to produce \( \text{occ}(\rho_i, y) \cap U_0 \), are considered by \( \mathbf{u}_{\mathbf{S}_{\mathbf{R}}} \) when it handles \( x_i = t_i \).

It remains to show that some of these sets are in \( \text{rel}(x_i, R_{i-1}) \) and some in \( \text{rel}(t_i, R_{i-1}) \). If this is the case, in fact, \( \mathbf{u}_{\mathbf{S}_{\mathbf{R}}} \) produces, among others, also the set \( \text{occ}(\rho_i, y) \cap U_0 \).
To this end, observe that $B$ contains at least one variable, call it $z_1$, that occurs in $\rho_{r_-1}(x_i)$ and at least one, call it $z_2$, that occurs in $\rho_{r_-1}(t_i)$, in fact, $\mu_1$ is a unifier of $\rho_{r_-1}(x_i = t_i)$ and thus $y$ must be on both sides of $\mu_1(\rho_{r_-1}(x_i = t_i))$. Two possible cases may apply to $z_1$:

- $\rho_{r_-1}(x_i) \equiv x_i \equiv z_1$. In this case, since $x_i \in U_0$, $x_i \in \text{occ}(\rho_{r_-1}, x_i) \cap U_0 \neq \emptyset$. Hence $\text{occ}(\rho_{r_-1}, x_i) \cap U_0$ will be in $\text{rel}(x_i, R_{r_-1})$.

- $\rho_{r_-1}(x_i) \not\equiv x_i$. In this case, $\text{occ}(\rho_{r_-1}, z_1) \cap U_0$ contains $x_i$ and thus this set is included in $\text{rel}(x_i, R_{r_-1})$ too.

A similar reasoning applies to $z_2$. This concludes the proof. □

6.5. Optimality

Let us turn now to the proof of optimality of the abstract unification. The idea behind the proof is that for each set $S$ in the result of an abstract unification $U_{Sh}(\{A_1, U_1\}, \{A_2, U_2\}, \delta)$ we may identify a pair of concrete substitutions $\sigma_1, \sigma_2$, represented by each of the two abstract states, such that the result of the concrete unification $u_{R_1}(\sigma_1, \sigma_2, \delta)$ is a substitution whose abstraction is $\{\{S, \emptyset\}, U_1 \cup U_2\}$. The substitutions $\sigma_1$ and $\sigma_2$ are defined according to the following idea. The set $S$ is obtained as the union of sets $\{B_1, \ldots, B_k\} \subseteq A_1 \cup A_2$. The case that $k = 1$ is simple. When $k > 1$ it must be that for each $i \in [1, k], B_i \cap \text{Var}(\delta) \neq \emptyset$. The substitutions $\sigma_1$ and $\sigma_2$ assign to each variable $x \in S$ a term containing new variables $w_{1_1}, \ldots, w_{1_n}$ that correspond to those sets in $\{B_1, \ldots, B_k\}$ that contain $x$. These terms are such that the unification of $Eq(\sigma_1) \cup Eq(\sigma_2) \cup Eq(\delta)$ causes the unification of all these new variables. Therefore, in an $mgu$ of $Eq(\sigma_1) \cup Eq(\sigma_2) \cup Eq(\delta)$ all the variables in $S$ are bound to terms containing the same new variable and only that one. On the contrary, variables not in $S$ will be bound to ground terms.

**Theorem 6.4.** The abstract unification $U_{Sh}$ is optimal with respect to $U_{Rs}$.

**Proof.** Let $\{A_1, U_1\}, \{A_2, U_2\} \in \text{Sharing}$ with $U_1 \cap U_2 = \emptyset$. Let also $R_0 = A_1 \cup A_2$ and $U_0 = U_1 \cup U_2$ and $\delta = \{x_1/t_1, \ldots, x_n/t_n\} \in \text{Subst}$ such that $\text{Var}(\delta) \subseteq U_0$. The claim is:

$$U_{Sh}(\{A_1, U_1\}, \{A_2, U_2\}, \delta) = \alpha_{R_0, Sh}(U_{Rs}(\gamma_{R_0, Rs}(\{A_1, U_1\}), \gamma_{Sh, Rs}(\{A_2, U_2\}, \delta)).$$

In the light of the correctness shown in Theorem 6.3, we only need to show the following point (A):

(A) $U_{Sh}(\{A_1, U_1\}, \{A_2, U_2\}, \delta) \subseteq Sh \gamma_{R_0, Sh}(U_{Rs}(\gamma_{Sh, Rs}(\{A_1, U_1\}), \gamma_{Sh, Rs}(\{A_2, U_2\}, \delta))$

Again, the notation introduced in Section 6.2 is used below. Let also for $i \in [1, 2], \{\Sigma_i, U_i\} = \gamma_{Sh, Rs}(\{A_i, U_i\})$. We will show the following statement (X) that immediately implies (A):

(X) $\forall S \in R_{\alpha}, there are \sigma_1, \sigma_2 \in \text{Subst}, such that:
(a) $\sigma_1 \in \Sigma_1, \sigma_2 \in \Sigma_2, and Var(\sigma_1) \cap Var(\sigma_2) = \emptyset$;
(b) $u_{R_0}(\sigma_1, \sigma_2, \delta)$ is successful;
(c) if $u_{R_0}(\sigma_1, \sigma_2, \delta) = \rho_{\sigma}$, then $\gamma_{Sh, Rs}(\{\rho_{\sigma}, U_0\}) = \{\{S\}, U_0\}$.^2

^2 Observe that, for the sake of simplicity, we do not show the empty set in the first component of $\{\{S\}, U_0\}$. This causes no problem and is done throughout this proof.
Recall from the notation of Section 6.2 that \( S = \bigcup K \), with \( K = \{B_1, \ldots, B_k\} \subseteq R_0 \).

The following additional notation is needed:

- for each \( B_i \in K \), let \( w_i \) be a distinct extra variable not in \( U_0 \);
- for each \( x \in S \), let \( B_x = \{B \mid B \in K, x \in B\} \); notice that, by the hypothesis that \( U_1 \cap U_2 = \emptyset \), if \( x \in U_i \) then \( \bigcup B_x \subseteq U_i \); in fact, we can partition \( K \) in two parts, \( K_1 = \{B_i \in K \mid B_i \subseteq U_1\} \) and \( K_2 \) defined analogously; notice also that for any \( x, y \in U_i \) we may have \( B_x \cap B_y \neq \emptyset \);
- \( N = \max\{|B_x| \mid x \in S\} \);
- fixing \( x \in S \), and letting \( B_x = \{B_{i_1}, \ldots, B_{i_h}\} \), then the new variables associated to these sets will be denoted, \( w_{i_1}, \ldots, w_{i_h} \).

The substitutions \( \sigma_1 \) and \( \sigma_2 \) will be defined through one substitution \( \rho_0 \) such that \( \text{supp}(\rho_0) = U_0 \); \( \sigma_1 \) and \( \sigma_2 \) can be recovered from \( \rho_0 \) by separating the bindings concerning \( U_1 \) from those concerning \( U_2 \); \( \text{var-range}(\rho_0) \) consists only of the extra variables \( w_i \). The substitution \( \rho_0 \) is defined in the following four points:

1. For each \( x \in S \cap \text{Var}(\delta) \) there are two cases to distinguish:
   (a) If \( x \in \text{var-range}(\delta) \), then
   \[
   \rho_0(x) = s \left( c(w_{i_1}, w_{i_1}), c(w_{i_2}, w_{i_2}), \ldots, c(w_{i_h}, w_{i_h}), c(w_{i_1}, w_{i_1}), \ldots, c(w_{i_1}, w_{i_1}) \right)
   \]
   \( l_h \) times \( \quad N - l_h \) times
   (b) If \( x \in \text{supp}(\delta) \), then \( x \equiv x_r \), for some \( r \in [1, n] \), i.e., \( x \) is the left-hand side of the \( r \)-th binding, \( x_r / t_r \), of \( \delta \). In this case, \( \rho_0(x) = \zeta(t_r) \), where for each \( y \in \text{Var}(t_r) \setminus S, \zeta(y) = a \), for some constant \( a \), whereas if \( y \in S \cap \text{Var}(t_r) \), \( \zeta(y) \) is as follows:
   \[
   \zeta(y) = s \left( c(w_{i_1}, w_{i_1}), c(w_{i_2}, w_{i_2}), \ldots, c(w_{i_h}, w_{i_h}), c(w_{i_1}, w_{i_1}), \ldots, c(w_{i_1}, w_{i_1}) \right)
   \]
   \( l_h \) times \( \quad N - l_h \) times

2. For each \( x \in S \setminus \text{Var}(\delta) \), \( \rho_0(x) = s(w_{i_1}, \ldots, w_{i_h}) \).

3. For each \( x \in \text{Var}(\delta) \setminus S \) there are two cases to consider:
   (a) if \( x \in \text{var-range}(\delta) \), then \( \rho_0(x) = a \)
   (b) if \( x \in \text{supp}(\delta) \), then \( x \equiv x_r \), for some binding \( x_r / t_r \) of \( \delta \). In this case, \( \rho_0(x) = \zeta_a(t_r) \), where \( \zeta_a \) binds to the constant \( a \) all variables in \( t_r \).

4. For each \( x \in U_0 \setminus (S \cup \text{Var}(\delta)) \), \( \rho_0(x) = a \), for some constant \( a \).

Now, it remains to verify that \( \rho_0 \) satisfies statement (X), i.e., that the bindings of \( \rho_0 \) can be partitioned into two substitutions \( \sigma_1 \in \Sigma_1 \) and \( \sigma_2 \in \Sigma_2 \) satisfying points (a) to (c).

**Proof of point (X.a).** Let \( \sigma_1 = \{x / t \in \rho_0 \mid x \in U_1\} \); \( \sigma_2 \) is defined similarly. Obviously, these two substitutions have disjoint \( \text{supp} \) sets. They have also disjoint \( \text{var-range} \) sets because for each \( x \) in \( U_1 \), \( \text{Var}(\rho_0(x)) \subseteq \{w_{i_1}, \ldots, w_{i_h}\} \) and each of these variables corresponds to a set in \( B_i \subseteq A_i \). Thus, for any \( y \in U_2 \), \( \text{Var}(\rho_0(y)) \cap \text{Var}(\rho_0(x)) = \emptyset \).

To see that \( \sigma_1 \in \Sigma_i \), it suffices to observe that the construction of \( \rho_0 \) yields the following point (Y):

\[
(Y) \quad \bigcup K_i \subseteq \text{supp} \left( \sigma_i \right), \text{ and the variables in } \bigcup K_i \text{ are exactly the variables not ground in } \sigma_i, \text{ and for each such variable } x, \text{Var}(\sigma_i(x)) = \{w_{i_1}, \ldots, w_{i_h}\}.
\]

From point (Y) it follows immediately that \( \exists \text{R}_{\text{RS}}([\{\sigma_i\}, U_i]) = [K_i, U_i] \subseteq [A_i, U_i] \), and thus \( \sigma_i \in \Sigma_i \).
Proof of point (X.b). Consider for each equation \((x_i = t_i) \in \text{Eq}(\delta)\), the two terms \(\rho_0(x_i)\) and \(\rho_0(t_i)\). In order to show that they are unifiable, we distinguish two cases:

1. One of them is ground: this may arise either when \(x_i \not\in S\) or when \(\text{Var}(t_i) \cap S = \emptyset\).
   - When \(x_i \not\in S\) (i.e., case 3(b) of the def. of \(\rho_0\)), by Fact 1 of Section 6.3, we have \(\text{Var}(t_i) \cap S = \emptyset\). Thus, \(\rho_0(t_i)\) is ground too, and, by definition of \(\rho_0\), it is identical to \(\rho_0(x_i)\).
   - The case \(\text{Var}(t_i) \cap S = \emptyset\) is analogous to the previous one.

2. Both terms are non-ground terms. In this case, the following points come easily from the definition of \(\rho_0\) above:
   - (Z1) the only variables in the equation \(\rho_0(x_i) = \rho_0(t_i)\) are extra variables \(w_i\);
   - (Z2) \(\rho_0(x_i)\) and \(\rho_0(t_i)\) differ only for having different variables in corresponding leaf positions;
   - (Z3) solving the equation \(\rho_0(x_i = t_i)\) causes only the unification of all the present variables with each other, leaving all variables free.

Thus, in both cases, the unification is successful.

Proof of point (X.c). Two cases are distinguished:

1. Case \(S \cap \text{Var}(\delta) = \emptyset\). Here, \(K = \{S\}\) and \(S \in A_i\) for some \(i \in [1, 2]\). Let us fix such an \(i\). By the proof of point (X.a), \(\tau_{\text{rs-sk}}(\{(\rho_0), U_0\}) = \{(S), U_0\}\). From the same proof, it follows also that in \(\rho_0\) only the variables in \(S\) are not ground, and that they all share only the (extra) variable \(w \not\in U_0\) corresponding to \(S\). Hence, \(\tau_{\text{rs-sk}}(\{(\rho_0), U_0\}) = \{(S), U_0\}\). Now, observe that, by point (X.b)(1), the equations \(\rho_0(x_i = t_i)\) are ground identities. This means that they are simply eliminated by the unification algorithm. Thus, \(\rho_n = \rho_0\), as expected.

2. Case \(S \cap \text{Var}(\delta) \neq \emptyset\). Let us examine the computation of \(\text{mgu} (\text{Eq}(\rho_0) \cup \text{Eq}(\delta))\). It is well-known that, in computing an (idempotent) \(\text{mgu}\) of a system of equations, we may consider the equations in any order. We consider the unification of \(\rho_0(\text{Eq}(\delta))\) first, and then we apply the computed \(\text{mgu}\) to \(\text{Eq}(\rho_0)\).
   - Point (Z1) above, shows that only extra variables occur in \(\rho_0(\text{Eq}(\delta))\);
   - Fact 2 of Section 6.3 implies that all the extra variables \(w_1, \ldots, w_k\) occur in \(\rho_0(\text{Eq}(\delta))\);
   - Fact 3 together with point (Z3) prove that, in the unification process, all the (extra) variables present in \(\rho_0(\text{Eq}(\delta))\) are unified in a single variable. Thus an \(\text{mgu}\) of \(\rho_0(\text{Eq}(\delta))\) is \(\mu = \{w_1/w_k, \ldots, w_{k-1}/w_k\}\). We can substitute \(\text{Eq}(\mu)\) to \(\rho_0(\text{Eq}(\delta))\) and continue the unification with \(\text{Eq}(\mu) \cup \text{Eq}(\rho_0)\);
   - Point (Y) guarantees that extra-variables \(w_i\) may appear only in the range of \(\rho_0\). Hence, by the definition of \(\mu\), \(\mu(\text{Eq}(\rho_0))\) is in solved form. It is also easy to see that \(\text{Eq}(\mu) \cup \mu(\text{Eq}(\rho_0))\) is in solved form. Thus, it represents an idempotent \(\text{mgu}\) of our initial system \(\text{Eq}(\rho_0) \cup \text{Eq}(\delta)\). The corresponding \(\text{mgu}\) is \(\rho_n = \mu \circ \rho_0\). From point (Y) and the definition of \(\mu\) it follows that in \(\rho_n\) exactly the variables of \(S\) are not ground and that they all share the extra variable \(w_k\), that is the only variable in \(\text{var-range} (\rho_n)\).

From the previous points, we get \(\tau_{\text{rs-sk}}(\{(\rho_n), U_0\}) = \{(S), U_0\}\) (recall that \(w_k \notin U_0\), and thus it is filtered out by the abstraction). This completes the proof of the the desired statement (X) and of the whole Theorem as well. \(\square\)
As a final remark, observe that $U_{S^0}$ is not complete. For instance, consider $U_1 = \{x\}$, $U_2 = \{z\}$, and let $\sigma = \{x/f(a,w)\}$, and $\delta = \{x/f(z,a)\}$. In this case, $\alpha_{R^0,S^0}(U_{R^0}(\{\sigma\}, U_1), \{\delta\}, U_2)$ is equal to $\{\emptyset\}, U_1 \cup U_2$, whereas the corresponding abstract unification $U_{S^0}(\{\{x\}, \emptyset\}, U_1), \{\{z\}, \emptyset\}, U_2, \delta)$ results to be equal to $\{\{x,z\}, \emptyset\}, U_1 \cup U_2$.

7. Conclusions and related works

Recently, several researchers have studied the domain Sharing and its operations. Codish et al. in Ref. [10] propose an alternative way of representing set-sharing information. In place of collecting the sets of variables that may share a common variable, as Sharing does, they associate to each variable the set of variables that may be contained in the terms bound to that variable. Clearly this new domain is isomorphic to Sharing. In Ref. [10] the abstract operations of this new domain are also discussed. The abstract unification is based on an associative commutative and idempotent equality theory. Abstract lub is shown to be complete, whereas only the correctness of the abstract unification and projection are shown (cf. Theorem 7 of Ref. [10]). In the light of the optimality result shown in the present paper, it is expectable that also the abstract unification of Ref. [10] can be proven optimal.

In Ref. [9] it is proved that a strict abstraction, $SS^0$, of Sharing is sufficient for computing pair-sharing. This means that, when analyzing programs, in place of using Sharing, we may use the more abstract $SS^0$ obtaining exactly the same pair-sharing information. This is important because abstract unification in $SS^0$ is polynomial whereas that in Sharing is exponential.

It is worth mentioning that, as Baghara et al. remark in Ref. [9], $SS^0$ is the quotient of Sharing with respect to pair-sharing, where the notion of quotient was introduced in Ref. [7].

In the light of the result of Baghara et al., it is natural to wonder whether there are analyses for which the Sharing domain is still needed or for all practical applications it can be replaced by the more efficient $SS^0$.

In order to answer this question, we need to explain briefly the relation between $SS^0$ and Sharing. For each element $[S, U] \in$ Sharing, the corresponding abstraction in $SS^0$ is $\rho(S), U)$, where, intuitively, $\rho(S)$ adds to $S$ every subset of $U$ that does not introduce any new pair-sharing to that already expressed by $S$.

Thus, for instance, $SS^0$ cannot distinguish between the following two values of Sharing: $S_1 = \{\{x,y\}, \{x,z\}, \{y,z\}\}, U$ and $S_2 = \{\{x,y\}, \{x,z\}, \{y,z\}, \{x,y,z\}\}, U$, where $U = \{x,y,z\}$. Observe in fact that:

$$\rho(\{x,y\}, \{x,z\}, \{y,z\}) = \rho(\{x,y\}, \{x,z\}, \{y,z\}, \{x,y,z\})$$

$$= \{\{x,y\}, \{x,z\}, \{y,z\}, \{x,y,z\}\}$$

Being able to distinguish between these two sharing situations may be important for optimizations concerning the AND parallel execution of Prolog programs. Assume we want to execute $p(x), q(y), r(z)$ by means of parallel processes. In situations rep-

\footnote{Observe that Sharing is also studied in [7], where its quotient with respect to groundness information is characterized as the well-known domain $Def$ consisting of definite propositional formulas.}
resented by $S_1$ we are sure that no variable is shared by more than two processes, whereas in the situations represented by $S_2$ all three processes may share a variable. Good strategies for deciding which goals should be solved in parallel might use such information.

Finally, it is interesting to observe that the relation between Sharing and pair-sharing has also been studied in Ref. [15], with a different goal: to use the complementation operation Ref. [8], in order to decompose the domain Sharing into three simpler domains, each expressing one of the different information that coexist in Sharing, namely, groundness, pair-sharing and set-sharing information. The reduced product of these three components gives Sharing back. It is worthwhile to mention that in that paper it is shown that Sharing cannot be obtained as the reduced product of a domain $PS$ expressing only pair-sharing with some other domain more abstract than Sharing. More precisely, in Ref. [15] it is shown that the complement of $PS$ with respect to Sharing is Sharing itself.

Acknowledgements

The work has been partially supported by the Italian MURST project 9701248444-044. Thanks to the anonymous referees for in-depth reading and helpful comments.

References


